

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-215171

(P2000-215171A)

(43)公開日 平成12年8月4日 (2000.8.4)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 E 2 C 0 0 6
B 4 2 D 15/10	5 0 1	B 4 2 D 15/10	5 0 1 L 5 B 0 8 6
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A 9 A 0 0 1 6 7 3 D

審査請求 未請求 請求項の数13 O.L (全 16 頁)

(21)出願番号 特願平11-18030

(71)出願人 000006108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(22)出願日 平成11年1月27日(1999.1.27)

(72)発明者 吉浦 裕

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 佐々木 良一

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 岩村 充

東京都練馬区中村2-14-17

(74)代理人 10008/170

弁理士 富田 和子

最終頁に続く

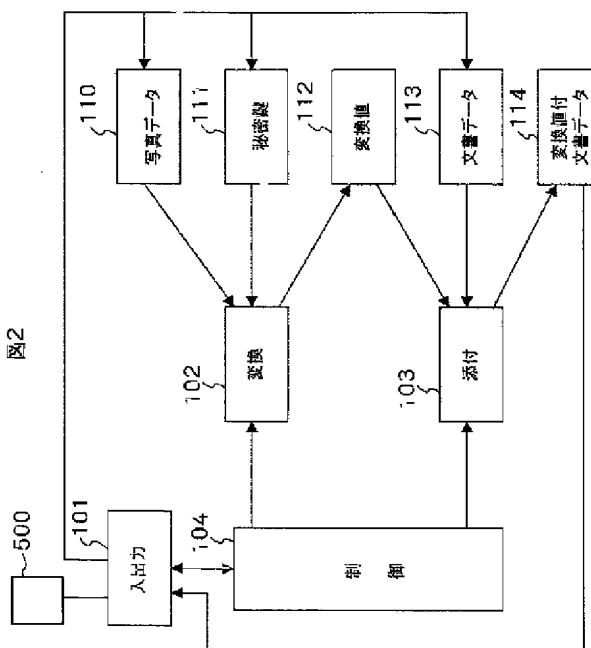
(54)【発明の名称】 認証システムおよび認証方法

(57)【要約】

【課題】偽造困難な身分証明書を実現する。

【解決手段】変換部102は対象者の顔写真の写真データ110、身分証明発行者の秘密鍵111で暗号化した変換値112を作成する。添付部103は、入出力部101を介して、変換値112を対象者の氏名住所などの文書データ113に添付した変換値付文書データを携帯可能な電子的な記録媒体500に記録する。記録媒体500は対象者に発行され、認証時には、記録媒体500に含まれる変換値を、身分証明発行者の公開鍵で復号した写真データの表す画像に写された人物と、記録媒体500の所持者が同一人物かどうかを判定する。

図2



【特許請求の範囲】

【請求項1】物理的個体を認証するための情報を記録した記録体を用いて物理的個体を認証する認証システムであって、
記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化した暗号情報を生成する手段と、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録する手段とを有する記録体作成装置と、前記記録体に記録された前記暗号情報を、前記秘密鍵と対の公開鍵で復号し、前記記録体によって認証可能とされた物理的個体の特徴値を復元する手段と、
復元された前記記録体によって認証可能とされた物理的個体の特徴値と、前記記録体によって認証可能とされていると称される物理的個体の前記特徴値とを比較する手段とを有することを特徴とする認証システム。

【請求項2】物理的個体を認証するための情報を記録した記録体を用いて物理的個体を認証する認証システムであって、

物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を蓄積するデータベースと、記録体によって認証可能とすべき物理的個体の前記特徴値を、前記データベースに格納すると共に、記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースから検索するための検索情報を生成する手段と、生成した検索情報を公開鍵暗号に従った秘密鍵で暗号化した暗号情報を生成する手段と、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録する手段とを有する記録体作成装置と、

前記記録体に記録された前記暗号情報を、前記秘密鍵と対の公開鍵で復号して検索情報を復元する手段と、復元された検索情報を用いて、前記記録体作成装置の前記データベースから、前記記録体によって認証可能とされた物理的個体の特徴値を検索する手段とを有する認証用装置とを有することを特徴とする認証システム。

【請求項3】請求項1または2記載の認証システムであって、

前記認証用装置は、特定の物理的個体の前記特徴値を取り込む手段と、前記記録体によって認証可能とされた物理的個体の特徴値とを比較し、比較結果を提示する手段を有することを特徴とする認証システム。

【請求項4】物理的個体を認証するための情報を記録した記録体を用いて物理的個体を認証する認証方法であって、

記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化した暗号情報を生成する手段と、

前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録する手段と、

前記記録体に記録された前記暗号情報を、前記秘密鍵と対の公開鍵で復号し、前記記録体によって認証可能とされた物理的個体の特徴値を復元する手段と、
復元された前記記録体によって認証可能とされた物理的個体の特徴値と、前記記録体によって認証可能とされていると称される物理的個体の前記特徴値とを比較する手段とを有することを特徴とする認証方法。

【請求項5】物理的個体を認証するための情報を記録した記録体を用いて物理的個体を認証する認証方法であって、

記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、前記データベースに格納すると共に、記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースから検索するための検索情報を生成する手段と、

生成した検索情報を公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成する手段と、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録する手段と、

前記記録体に記録された前記暗号情報を、前記秘密鍵と対の公開鍵で復号して検索情報を復元する手段と、復元された検索情報を用いて、前記記録体作成装置の前記データベースから、前記記録体によって認証可能とされた物理的個体の特徴値を検索する手段と、

検索した前記記録体によって認証可能とされた物理的個体の特徴値と、前記記録体によって認証可能とされていると称される物理的個体の前記特徴値とを比較する手段とを有することを特徴とする認証方法。

【請求項6】物理的個体を認証するための情報を記録した記録体を作成する記録体作成装置であって、

記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化した暗号情報を生成する手段と、

前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録する手段とを有することを特徴とする記録体作成装置。

【請求項7】物理的個体を認証するための情報を記録した記録体を作成する記録体作成装置であって、

物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を蓄積するデータベースと、記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースに格納すると共に、記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースから検索するための検索情報を生成する手段と、

生成した検索情報を公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成する手段と、

前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録する手段とを有することを特徴とする記録体作成装置。

【請求項8】物理的個体を認証するための情報を記録した記録体を作成する方法であって、記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成するステップと、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録するステップとを有することを特徴とする方法。

【請求項9】物理的個体を認証するための情報を記録した記録体を作成する方法であって、記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、データベースに格納すると共に、記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースから検索するための検索情報を生成するステップと、

生成した検索情報を公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成する手段と、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録するステップとを有することを特徴とする方法。

【請求項10】電子計算機に読み込まれ実行されるプログラムを記憶した記憶媒体であって、

前記プログラムは、前記電子計算機に、物理的個体を認証するための情報を記録した記録体を作成させるプログラムであって、かつ、前記プログラムは、記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成するステップと、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情報を前記記録体に記録するステップとを前記電子計算機に実行させるプログラムであることを特徴とする記憶媒体。

【請求項11】電子計算機に読み込まれ実行されるプログラムを記憶した記憶媒体であって、

前記プログラムは、前記電子計算機に、物理的個体を認証するための情報を記録した記録体を作成させるプログラムであって、かつ、前記プログラムは、記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、データベースに格納すると共に、記録体によって認証可能とすべき物理的個体の前記特徴値を前記データベースから検索するための検索情報を生成するステップと、生成した検索情報を公開鍵暗号に従った秘密鍵で暗号化し暗号情報を生成するステップと、前記暗号情報および当該記録体によって認証可能とすべき物理的個体について証する情

報を前記記録体に記録するステップとを前記電子計算機に実行させるプログラムであることを特徴とする記憶媒体。

【請求項12】物理的個体を認証するための情報を記録した記録体であって、

記録体によって認証可能とする物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化した暗号情報を記録した領域と、当該物理的個体について証する情報が記録された領域とを有することを特徴とする記録体。

【請求項13】物理的個体を認証するための情報を記録した記録体であって、

データベースに格納された、記録体によって認証可能とする物理的個体の前記特徴の値を検索するための検索情報を公開鍵暗号に従った秘密鍵で暗号化した暗号情報を記録した領域と、当該物理的個体について証する情報が記録された領域とを有することを特徴とする記録体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、人物を認証するための情報が記述された身分証明書などの、何らかの物理的個体を認証するための情報が記述された記録体に関するものであり、特に、その偽造を防止する技術に関するものである。

【0002】

【従来の技術】物理的個体を認証するための情報が記録された記録体としては、運転免許証や、パスポート、社員証などの各種身分証明書、各種鑑定書などがある。これらは、物理的個体を認証するための文字や写真による情報を、紙や紙に準じる物体に直接視認可能なように印刷や筆書などの方法により記録したものである。

【0003】また、多くの場合、物理的個体を認証するための情報は、物理的個体を特定するための情報と、その物理的個体について証される情報よりなる。たとえば、パスポートには、物理的個体を特定するための情報として顔写真が貼付され、物理的個体について証される情報として人物の氏名、住所、生年月日、国籍などが記録される。

【0004】物理的個体を認証するものは、記録媒体に記録された物理的個体を特定するための情報によって物理的個体を特定し、特定した物理的個体について、記録媒体に記録された物理的個体について証される情報を認証する。たとえば、パスポートであれば、空港に配置される入出国管理官などの認証者は、パスポートに貼付られた顔写真とパスポートの所持者の人相が一致する場合に、パスポートの所持者がパスポートに記録されている氏名、住所、生年月日、国籍などを持つ人間であることを認証する。

【0005】

【発明が解決しようとする課題】さて、これら運転免許

証や、パスポート、社員証などの各種身分証明書、各種鑑定書などは、犯罪目的のために偽造の対象となることがある。たとえば、パスポートであれば、偽造パスポートは密入国や密輸や犯罪者の渡航などに使用されることがある。したがって、これら偽造を防止することは、社会的な要請である。

【0006】これら偽造を防止するために今まで々な工夫が成されてきているが、その度に偽造も巧妙を極め、未だ、決定的な対策が見いだされていないのが現状である。特に、正規のパスポートの顔写真の貼り換えによる偽造は、その発見が容易でないことより大きな問題となっている。

【0007】そこで、本発明は、偽造、特に、パスポートの顔写真などの、物理的個体を特定するための情報の偽造をより効果的に防止することができる、物理的個体を認証するための情報を記録した記録体を提供することを課題とする。

【0008】

【課題を解決するための手段】前記課題達成のために、本発明は、たとえば、物理的個体を認証するための情報を記録した記録体を用いて物理的個体を認証する認証システムであって、記録体によって認証可能とすべき物理的個体の、個々の物理的個体を識別するために用いることのできる特徴値を、公開鍵暗号に従った秘密鍵で暗号化した暗号情報を生成する手段と、前記暗号情報および物理的個体について証する情報を前記記録体に記録する手段とを有する記録体作成装置と、前記記録体に記録された前記暗号情報を、前記秘密鍵と対の公開鍵で復号し、前記記録体によって認証可能とされた物理的個体の特徴の値を復元する手段とを有する認証用装置とを有することを特徴とする認証システムを提供する。

【0009】このような認証システムによれば、記録体によって認証可能とすべき物理的個体を特定する情報として、単なる物理的個体の写真などの物理的個体の特徴値ではなく、所定の秘密鍵で暗号化した物理的個体の特徴値を記録する。そして、認証時には、暗号化に用いた秘密鍵と対の公開鍵で復号した特徴値と、記録体によって認証されると称される物理的個体の特徴値との比較によって、物理的個体を認証する。ここで、このような公開鍵で復号した場合に偽の物理的個体の特徴値となるデータを偽造することは、対の秘密鍵を知らない限り極めて困難であり、かつ、秘密鍵を公開鍵や秘密鍵で暗号化された特徴値から導くことも極めて困難である。したがって、物理的個体を特定するための情報を偽造をより効果的に防止することができる認証用の記録体を提供することができる。

【0010】なお、前記物理的個体は人間であって、前記個々の物理的個体を識別するために用いることのできる物理的個体の特徴は、人間の身体的特徴であってよい。また、前記物理的個体の特徴を人間の身体的特徴と

した場合において、前記記録体によって認証可能とする物理的個体を写した画像を、当該記録体によって認証可能とする前記物理的個体の特徴値として用いるようにしてよい。

【0011】

【発明の実施の形態】以下、本発明の実施形態を、物理的個体を認証するための情報を記録した記録体が、身分証明を行う記録体であるところの身分証明体である場合を例にとり説明する。

【0012】

【0013】図1に、本第1実施形態に係る認証システムの構成を示す。

【0014】図示するように、本認証システムは、身分証明体を発行する1または複数の発行側装置100と、身分証明体に基づいて身分を認証する1または複数の認証側装置200を備える。ここで、本第1実施形態に係る身分証明体は、電子データを記憶する、携帯型の電子的記録媒体であり、例えば、メモリカードやICカードや磁気カードなどの電子カードである。

【0015】図2に示すように、発行側装置100は、入出力部101と制御部104と変換部102と添付部103を有している。入出力部101は、身分証明体500によって身分を保証される者（以下、「被保証者と呼ぶ」）の顔の画像データである写真データ110、身分証明体500によって被保証者の身分を保証する者又は機関（以下、「保証者」と呼ぶ）の秘密鍵111、被保証者の氏名や住所や生年月日などの身分証明体500によって保証する被保証者についての事項を記述した文書データ113を発行側装置100に取り込む。また、入出力部101は、身分証明体500に後述する変換値付文書データ114を記録する。また、変換部102は、写真データ110を秘密鍵111で暗号化した変換値112を作成する。添付部103は、文書データ113に変換値112を添付し、前述した変換値付文書データ114を作成する。制御部104は、入出力部101と変換部102と添付部103の以上の動作を制御する。

【0016】ただし、発行側装置100は、図3に示すように、実際には、CPU301や、主記憶302、ハードディスク装置である外部記憶装置303a、他の外部記憶装置である303b、通信制御装置304、キーボードやポインティングデバイスなどの入力装置305、表示装置などの出力装置306、画像データを取り込む画像入力装置308、身分証明体であるところの電子カードへの書き込みを行なう電子カード書き込み装置309などを備えた、電子計算機上に構築することができる。ここで、画像入力装置308は、被保証者を撮影した写真から画像を取り込むものであっても、直接、被保証者を撮影し、その画像を取り込むものであってもよい。

【0017】この場合、図2の入出力部201と制御部204と変換部202と添付部203は、CPU301が主記憶302にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。このプログラムは、予め、外部記憶装置303aに記憶され、必要に応じて主記憶302にロードされ、CPU301によって実行される。または、可搬型の記憶媒体307、たとえば、CD-ROMを扱う外部記憶装置303bもしくは通信制御装置204を介して、直接、必要に応じて、可搬型の記憶媒体307もしくはネットワークから主記憶302にロードされ、CPU301によって実行されるか、もしくは、一旦、ハードディスク装置などの外部記憶装置303a上にインストールされた後、必要に応じて主記憶302にロードされ、CPU301によって実行される。

【0018】次に、図4に示すように、認証側装置200は、撮影部201、入出力部202、制御部203、変換部204、比較部205を有する。

【0019】入出力部213は、保証者の公開鍵211を取り込んだり、撮影部201を介して被保証者を自称する者の顔の画像データであるところの顔画像データ213を取り込んだり、身分証明体500に記憶された変換値付文書データ210を取り込んだりする。また、入出力部213は、後述する比較部205の比較結果や、写真データ212の表す画像や、変換値付文書データ210に含まれる文書データの表示も行う。変換部204は、変換値付文書データ210に含まれている保証者の秘密鍵で暗号化された被保証者の写真データ212を、保証者の公開鍵で復号することにより被保証者の写真データ212を復元する。比較部205は、写真データ212と顔画像データ213をパターンマッチングの手法などにより比較し、所定程度以上両者が類似しているかどうかを比較結果として算出する。制御部203は、撮影部201、入出力部202、変換部204、比較部205の以上の動作を制御する。

【0020】ただし、図5に示すように、認証側装置200も、実際には、CPU401や、主記憶402、ハードディスク装置である外部記憶装置403a、他の外部記憶装置である403b、通信制御装置404、キーボードやポインティングデバイスなどの入力装置405、表示装置などの出力装置406、画像データを取り込む画像入力装置408、身分証明体であるところの電子カードの読み出し行う電子カード読み取り装置409などを備えた、電子計算機上に構築することができる。ここで、画像入力装置408は、被保証者を自称する者を撮影した写真から画像を取り込むものであっても、直接、被保証者を自称する者を撮影し、その画像を取り込むものであってもよい。

【0021】この場合、図4の撮影部201、入出力部202、制御部203、変換部204、比較部205

は、CPU401が主記憶402にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。このプログラムは、予め、外部記憶装置303aに記憶され、必要に応じて主記憶402にロードされ、CPU401によって実行される。または、可搬型の記憶媒体407、たとえば、CD-ROMを扱う外部記憶装置403bもしくは通信制御装置404を介して、直接、必要に応じて、可搬型の記憶媒体407もしくはネットワークから主記憶402にロードされ、CPU401によって実行されるか、もしくは、一旦、ハードディスク装置などの外部記憶装置403a上にインストールされた後、必要に応じて主記憶402にロードされ、CPU401によって実行される。

【0022】以下、本第1実施形態に係る認証システムの動作について説明する。

【0023】まず、本第1実施形態において利用する公開鍵暗号技術について簡単に説明する。

【0024】公開鍵暗号技術は、インターネットを利用した通信などにおいて広く用いられている技術であり、この技術では、まず、 $g(f(n, S), V) = n, f(g(n, V), S) = n$ が成立する秘密鍵S、公開鍵Vの組を作成する。ここでnは任意のデータ、f、gは所定の関数であり、上記式は、秘密鍵Sを用いて暗号化した任意のデータは公開鍵Vを用いて復号化することができ、また、逆に、公開鍵Vを用いて暗号化した任意のデータは秘密鍵Sで復号化できることを表している。また、ここで、公開鍵Vから秘密鍵Sを求めるることは実質的に不可能となっている。

【0025】ここで、秘密鍵S、公開鍵Vを作成したならば、作成者は公開鍵Vを、相手方に渡し、秘密鍵Sは作成者が秘密に保持する。

【0026】そして、相手方が鍵の作成者にデータを送る場合、データを公開鍵Vで暗号化したものを鍵の作成者に渡す。そして、データを受け取った鍵の作成者は、データを秘密鍵Sを用いて復号化する。また、その逆の処理も可能である。つまり、鍵の作成者が、相手方にデータを送る場合には、データを秘密鍵Sで暗号化したものを相手方に渡す。そして、データを受け取った相手方は、データを公開鍵Vを用いて復号化する。

【0027】ただし、実用上、安全を確保できる長さの秘密鍵を用いた暗号化や、公開鍵を用いた復号化の処理には時間を要するため、一般的には、相手方（あるいは鍵の作成者）が、鍵の作成者（あるいは相手方）にデータを送る場合には、データを一時鍵で暗号化したものと、この一時鍵を公開鍵V（あるいは秘密鍵S）で暗号化したものを鍵の作成者（あるいは相手方）に渡し、データを受け取った鍵の作成者（あるいは相手方）は、一時鍵を秘密鍵S（あるいは公開鍵V）を用いて復号化し、この一時鍵を用いてデータを復号するというように2段階の暗号化が行われている。

【0028】また、このようなデータの暗号化の技術と共に、鍵の保持者がデータの特徴値を秘密鍵で暗号化したものと、暗号化したデータに添付し送ることにより、データを受け取ったものが、公開鍵で復号した特徴値を受け取ったデータの実際の特徴値の比較によって、データの真正性を認証可能とする、電子署名として知られる技術が用いられることが多い。この場合、データの特徴値としては一方方向ハッシュ関数によるデータの評価値などの一方方向関数による評価値が通常用いられる。一方方向関数は、実質上、データから関数で評価した評価値を算出可能であるが、評価値から元のデータを算出することは実質的に実用上不可能である性質をもつ。

【0029】以上、公開鍵暗号について説明した。

【0030】次に、発行側装置100の動作について説明する。

【0031】図6に、発行側装置100の制御部104が行う処理の手順を、図7にその処理のようすを示す。ただし、図7は、本処理の理解を容易ならしめるために、データの構成を模式的に示したものである。

【0032】ここでは、予め、保証者の秘密鍵111が入出力部101を介して発行側装置100内に取り込まれ、記憶されているものとする。

【0033】さて、図示するように、ある被保証者の身分保証体500を発行する場合、制御部104は、まず、入出力部101を制御し、被保証者の写真データ110と被保証者の氏名や住所や生年月日などを記述した文書データ113を取り込む（ステップ601）。

【0034】次に、変換部102を制御し、図7に示すように、前述した公開鍵暗号技術に従って写真データ110を秘密鍵111で暗号化した変換値112を作成させる（ステップ602）。そして、最後に、添付部103を制御し、文書データ113に変換値112を添付した変換値付文書データ114を作成し、入出力部101を介して、身分保証体500に書き込む（ステップ603）。

【0035】さて、このようにして変換値付文書データ114が記録された身分保証体500は、被保証者に渡され、被保証者によって携帯され、被保証者の身元の認証が必要なときに、被保証者によって提示される。

【0036】次に、認証側装置200の動作について説明する。

【0037】図8に、認証側装置200の制御部203が行う処理の手順を、図9にその処理のようすを示す。ただし、図9は、本処理の理解を容易ならしめるために、データの構成を模式的に示したものである。

【0038】ここでは、予め、保証者の秘密鍵111が入出力部202を介して認証側装置200内に取り込まれ、記憶されているものとする。

【0039】図示するように、被保証者を自称するものから、その者が携帯する身分保証体500の提示を受け

ると、認証側装置200の制御部203は、まず、入出力部202を介して身分保証体500から、変換値付文書データ210を取り込む（ステップ801）。そして、変換部204を制御し、保証者の公開鍵802で、変換値付文書データ210に含まれている保証者の秘密鍵で暗号化された被保証者の写真データ212を、前述した公開鍵暗号技術に従って保証者の公開鍵で復号することにより被保証者の写真データ212を復元させる（ステップ802）。

【0040】次に、撮影部201、入出力部202を制御し、被保証者を自称する者の顔の画像を顔画像データ213として取り込む（ステップ803）。そして、比較部205を制御し、顔画像データ213と復号した写真データ212とをパターンマッチングの手法などにより比較し、所定程度以上両者が類似しているかどうかを比較結果として算出し、入出力部202を介して、比較結果を、復号した写真データ212が表す画像や変換値付文書データ210に含まれる文書データが示す文書と共に表示する（ステップ804）。ここで、顔画像データ213と復号した写真データ212と所定程度以上両者が類似している場合に、比較結果は、この被保証者を自称している者が確かに被保証者であって、身分保証体500が確かに、この被保証者に対して発行されたものであることが認証された旨を示すことになる。

【0041】以上、本発明の第1の実施形態について説明した。以上のように、本第1実施形態によれば、被保証者を特定する情報として、単なる被保証者の写真データではなく、保証者の秘密鍵で暗号化した被保証者の写真データを身分保証体に記録し、保証者の公開鍵で復号した写真データと被保証者を自称する者の顔との比較によって、被保証者を認証する。ここで、このような保証者の公開鍵で復号した場合に不正者の写真データとなるデータを偽造することは、保証者の秘密鍵を知らない限り極めて困難であり、かつ、保証者の秘密鍵を公開鍵や秘密鍵で暗号化された写真データから導くことも極めて困難である。したがって、本第1実施形態によれば、被保証者を特定するための情報を偽造をより効果的に防止することができる身分保証体を提供することができる。

【0042】なお、以上の実施形態では、発行側装置100において、被保証者の写真データだけを保証者の秘密鍵を用いて暗号化したが、被保証者の氏名や従者や生年月日などの身分保証体が保証する被保証者についての事項を記述した文書データも保証者の秘密鍵を用いて暗号化して身分保証体に記録するようにし、認証側装置200において保証者の公開鍵で文書データを復号して利用するようにしてもよい。このようにすることにより、身分保証体が保証する被保証者についての事項についても、写真データと同様に、より効果的に偽造を防止することができるようになる。

【0043】また、以上の実施形態では、認証側装置2

00において、被保証者を自称する者の顔画像データと、身分保証体に記録された保証者の秘密鍵によって暗号化された写真データを復号した画像を比較し、比較結果を表示したが、この比較は行わないようにしてもよい。すなわち、認証側装置200は、身分保証体に記録された保証者の秘密鍵によって暗号化された写真データを復号した画像と、身分保証体に記録された文書データの表示のみを行い、認証側装置200を利用する認証者が、表示された画像と、被保証者を自称する者とを見比べ、被保証者を自称する者が、復号した写真データが表す画像に写された人物と同一人物であるかどうかを判断するようにしてもよい。

【0044】また、以上の実施形態において、身分保証体には保証者の秘密鍵によって暗号化された写真データのみ記録し、被保証者の氏名や従者や生年月日などの身分保証体が保証する被保証者についての事項は身分保証体と分離不可能な形態で、直接視認可能なように記録するようにしてもよい。例えば、身分保証体である電子カードの表面に偽造が困難な形態で文字を印刷やエッチングなどの手法により記録するようにしてもよい。

【0045】以下、本発明の第2の実施形態について説明する。

【0046】図10に本第2実施形態に係る認証システムの構成を示す。

【0047】図示するように、本第2実施形態に係る認証システムはネットワーク6000を介して接続される、1以上のセンタ装置1000と、1以上の認証側装置2000を有する。

【0048】ここで、本第2実施形態に係る身分証明体は、印刷などの直接視認可能な形態によって文字や図形などが記録される記録媒体であり、例えば、紙やプラスチックや金属のカードである。

【0049】さて、図11に示すようにセンタ装置1000は、入出力部1001と制御部1002とデータベース管理部1003と変換部1004と添付部1005とを有している。入出力部1001は、被保証者の顔の画像データである写真データ1006、保証者の秘密鍵1009、被保証者の氏名や住所や生年月日などの身分証明体500によって保証する被保証者についての事を記述した文書データ1111を取り込む。また、入出力部1001は、身分証明体500に後述する変換値付文書データ1112を印刷によって記録する。

【0050】また、データベース管理部1003は、写真データのデータベース1007を管理しており、入出力部1001が取り込んだ写真データ1006に登録番号1008を与えた上でデータベース1007に登録する。ここで登録番号1008には、写真データ1006を登録したセンタ装置1000を識別するための番号を含めるようにする。変換部1004は、写真データ1006の登録番号1008を秘密鍵1009で暗号化した変

換値1010を作成する。添付部1005は、文書データ1111に、変換値1010をバーコードによって表した图形を挿入し、前述した変換値付文書データ1112を作成する。

【0051】ここで、入出力部1001はネットワーク6000を介して認証側装置2000から送られた、登録番号を伴う検索要求を取り込みデータベース管理部1003に送る。データベース管理部1003は、検索要求に伴う登録番号の写真データをデータベース1007から検索し、入出力部1001に送る。入出力部1001は、送られた写真データを、ネットワーク6000を介して検索要求を発行した認証側装置2000に送信する。

【0052】制御部1002は、入出力部1001とデータベース管理部1003と変換部1004と添付部1005の以上の動作を制御する。

【0053】ただし、センタ装置1000は、図12に示すように、実際には、CPU3001や、主記憶3002、ハードディスク装置である外部記憶装置3003a、他の外部記憶装置である3003b、ネットワーク6000に接続する通信制御装置3004、キーボードやポインティングデバイスなどの入力装置3005、表示装置などの出力装置3006、画像データを取り込む画像入力装置3008、身分証明体であるところのカード500への印刷を行う印刷システム3009などを備えた、電子計算機上に構築することができる。ここで、画像入力装置3008は、被保証者を撮影した写真から画像を取り込むものであっても、直接、被保証者を撮影し、その画像を取り込むものであってもよい。

【0054】この場合、図11の入出力部1001と制御部1002とデータベース管理部1003と変換部1004と添付部1005とは、CPU3001が主記憶3002にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。このプログラムは、予め、外部記憶装置3003aに記憶され、必要に応じて主記憶3002にロードされ、CPU3001によって実行される。または、可搬型の記憶媒体3007、たとえば、CD-ROMを扱う外部記憶装置3003bもしくは通信制御装置3004を介して、直接、必要に応じて、可搬型の記憶媒体3007もしくはネットワークから主記憶3002にロードされ、CPU3001によって実行されるか、もしくは、一旦、ハードディスク装置などの外部記憶装置3003a上にインストールされた後、必要に応じて主記憶3002にロードされ、CPU3001によって実行される。

【0055】次に、図13に示すように、認証側装置2000は、入出力部2001、制御部2002、変換部2003、リモート検索部2004を有する。

【0056】入出力部2001は、保証者の公開鍵2006を取り込んだり、身分証明体5000に印刷された

バーコードが表す数値を変換値2005として取り込んだりする。また、入出力部2001は、リモート検索部2004が発行する検索要求をネットワーク6000を介してセンタ装置1000に送信すると共に、検索要求の応答として、センタ側装置1000から送られた写真データをリモート検索部2004に渡す。また、入出力部2001は、リモート検索部2004が検索した写真データの表す画像の表示も行う。

【0057】変換部2003は、変換値2005を、保証者の公開鍵で復号することにより写真データの登録番号2007を復号する。リモート検索部2004は、復号された登録番号を伴う検索要求を入出力部2001を介して、登録番号に含まれる番号より特定されるセンタ装置1000に発行することにより、センタ装置1000のデータベース1007から、この登録番号の写真データ入手し、入手した写真データを表示のために入出力部2001に渡す。

【0058】制御部2002は、入出力部2001、変換部2003、リモート検索部2004の以上の動作を制御する。

【0059】ただし、図14に示すように、認証側装置2000も、実際には、CPU4001や、主記憶4002、ハードディスク装置である外部記憶装置4003a、他の外部記憶装置である4003b、ネットワーク6000に接続する通信制御装置4004、キーボードやポインティングデバイスなどの入力装置4005、表示装置などの出力装置4006、身分証明体であるところのカード5000に印刷されたバーコードを読み取るバーコード読み取り装置4009などを備えた、電子計算機上に構築することができる。

【0060】この場合、図13の入出力部2001、制御部2002、変換部2003、リモート検索部2004とは、CPU4001が主記憶4002にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。このプログラムは、予め、外部記憶装置4003aに記憶され、必要に応じて主記憶4002にロードされ、CPU4001によって実行される。または、可搬型の記憶媒体4007、たとえば、CD-ROMを扱う外部記憶装置4003bもしくは通信制御装置4004を介して、直接、必要に応じて、可搬型の記憶媒体4007もしくはネットワークから主記憶4002にロードされ、CPU4001によって実行されるか、もしくは、一旦、ハードディスク装置などの外部記憶装置4003a上にインストールされた後、必要に応じて主記憶4002にロードされ、CPU4001によって実行される。

【0061】以下、本第2実施形態に係る認証システムの動作について説明する。

【0062】まず、センタ装置1000の動作について説明する。

【0063】図15に、センタ装置1000の制御部1002が行う処理の手順を、図16にその処理のようすを示す。

【0064】ここでは、予め、保証者の秘密鍵1009が入出力部1001を介してセンタ装置1000内に取り込まれ、記憶されているものとする。

【0065】さて、図示するように、ある被保証者の身分保証体5000を発行する場合、制御部1002は、まず、入出力部1001を制御し、被保証者の写真データ1006と被保証者の氏名や住所や生年月日などを記述した文書データ1011を取り込む（ステップ1501）。

【0066】次に、データベース管理部1003を制御し、図16に示すように、取り込んだ写真データ1006に、自センタ装置を識別するための番号を含めた登録番号を与え、登録番号と共に、データベース1007に登録する（ステップ1502）。

【0067】そして、変換部1004を制御し、前述した公開鍵暗号技術に従って写真データ1006をデータベース1007に登録した登録番号を、秘密鍵1009で暗号化し変換値112を作成させる（ステップ1503）。そして、最後に、添付部1005を制御し、文書データ1011が表す文書に変換値112をバーコード化した图形を挿入した文書を表す変換値付文書データ1012を作成し、入出力部1001を介して、変換値付文書データ1012の表す文書を身分保証体5000に印刷する（ステップ1504）。

【0068】さて、このようにして変換値付文書が記録された身分保証体5000は、被保証者に渡され、被保証者によって携帯され、被保証者の身元の認証が必要なときに、被保証者によって提示される。

【0069】また、制御部1002は、前述したように、入出力部1001がネットワーク6000を介して認証側装置2000から送られた、登録番号を伴う検索要求を受け取った場合に、データベース管理部1003を制御し、検索要求に伴う登録番号の写真データをデータベース1007から検索させ、入出力部1001に検索された写真データを、ネットワーク6000を介して検索要求を発行した認証側装置2000に送信させる。

【0070】次に、認証側装置2000の動作について説明する。

【0071】図17に認証側装置2000の制御部2002が行う処理の手順を、図18にその処理のようすを示す。

【0072】ここでは、予め、保証者の公開鍵2006が入出力部2001を介して認証側装置2000内に取り込まれ、記憶されているものとする。

【0073】図示するように、被保証者を自称するものから、その者が携帯する身分保証体5000の提示を受けると、認証側装置2000の制御部2002は、まず、

入出力部2001を介して身分保証体5000に印刷されたバーコードを読み取り、これを数値に変換し、変換値2005とする（ステップ1007）。

【0074】次に、変換部2003を制御し、変換値2005を、保証者の公開鍵2006で、前述した公開鍵暗号技術に従って復号することにより登録番号2007を復元させる（ステップ1702）。そして、リモート検索部2004を制御し、入出力部2001を介して、復元された登録番号2007を伴う検索要求を、登録番号2007に含まれる番号で特定されるセンタ装置1000に発行させ、この登録番号2007でセンタ装置1000のデータベースに登録された写真データを入手させ（ステップ1703）、入手した写真データが表す画像を入出力部2001において表示させる（ステップ1704）。

【0075】認証装置2000を利用する認証者は、この表示された画像と、被保証者を自称する者とを見比べ、被保証者を自称する者が、復号した写真データが表す画像に写された人物と同一人物であるかどうかを判断する。

【0076】以上、本発明の第2の実施形態について説明した。本第2実施形態によれば、写真データを暗号化したものに換えて、写真データの登録番号を暗号化したものを身分保証体に記録するので、前記第1実施形態に効果に加え、身分保証体に記録する情報量が少なくて済むという効果がある。このため、バーコードなどの印刷などの手法によって、紙などの非電子的な記録媒体にも、被保証者を特定する情報を記録することができる。また、登録番号より認証装置2000において、この登録番号の写真データを登録しているセンタ装置1000を識別可能としているので、複数のセンタ装置1000を設けるなど、柔軟な運用が可能となる。

【0077】なお、以上の第2実施形態では、写真データの登録番号を暗号化したものをバーコードとして身分証明体に記録したが、これは写真データの登録番号を暗号化したもの直接数値によって身分証明体に記録するようにしてもよい。また、身分証明体を電子的な記録媒体として、写真データの登録番号を暗号化したもの電子的に記録するようにしてもよい。

【0078】また、本第2実施形態においても前記第1実施形態と同様に、認証側装置2000において、被保証者を自称する者の顔画像データを取り込みと、身分保証体に記録された保証者の秘密鍵によって暗号化された登録番号によって検索した写真データとを比較し、比較結果を表示するようにしてもよい。

【0079】以上、本発明の実施形態について説明した。

【0080】なお、以上の実施形態では、被保証者の写真データを被保証者を特定するための情報とし、その暗号値もしくはその登録番号の暗号値を身分証明体に記録

したが、写真データに代えてもしくは写真データと組み合わせて、被保証者の指紋、声紋、虹彩パターン、網膜パターン、身長値、体重値、遺伝子パターン、血液情報などの他の、被保証者を特徴づける情報を単独でもしくは組み合わせて用い、その暗号値もしくはその登録番号の暗号値を身分証明体に記録するようにしてもよい。

【0081】

【発明の効果】以上のように、本発明によれば、偽造、特に、パスポートの顔写真などの、物理的個体を特定するための情報の偽造をより効果的に防止することができる、物理的個体を認証するための情報を記録した記録体を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1実施形態に係る認証システムの構成を示すブロック図である。

【図2】本発明の第1実施形態に係る発行側装置の構成を示すブロック図である。

【図3】本発明の第1実施形態に係る発行側装置のハードウェア構成例を示すブロック図である。

【図4】本発明の第1実施形態に係る認証側装置の構成を示すブロック図である。

【図5】本発明の第1実施形態に係る認証側装置のハードウェア構成例を示すブロック図である。

【図6】本発明の第1実施形態に係る発行側装置の行う処理の手順を示すフローチャートである。

【図7】本発明の第1実施形態に係る発行側装置の行う処理のようすを示した図である。

【図8】本発明の第1実施形態に係る認証側装置の行う処理の手順を示すフローチャートである。

【図9】本発明の第1実施形態に係る認証側装置の行う処理のようすを示した図である。

【図10】本発明の第2実施形態に係る認証システムの構成を示すブロック図である。

【図11】本発明の第2実施形態に係るセンタ装置の構成を示すブロック図である。

【図12】本発明の第2実施形態に係るセンタ装置のハードウェア構成例を示すブロック図である。

【図13】本発明の第2実施形態に係る認証側装置の構成を示すブロック図である。

【図14】本発明の第2実施形態に係る認証側装置のハードウェア構成例を示すブロック図である。

【図15】本発明の第2実施形態に係るセンタ装置の行う処理の手順を示すフローチャートである。

【図16】本発明の第2実施形態に係るセンタ装置の行う処理のようすを示した図である。

【図17】本発明の第2実施形態に係る認証側装置の行う処理の手順を示すフローチャートである。

【図18】本発明の第2実施形態に係る認証側装置の行う処理のようすを示した図である。

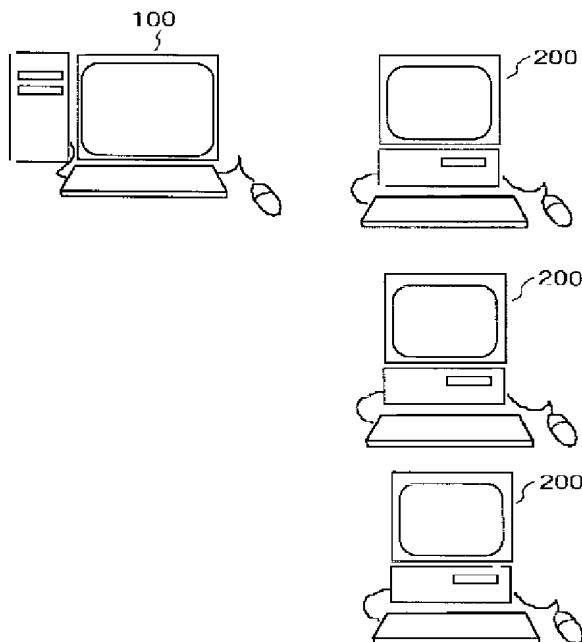
【符号の説明】

100 発行側装置、101 入出力部、104 制御部、102 変換部、103 添付部、200 認証側装置、201 撮影部、202 入出力部、203 制御部、204 変換部、205 比較部、500 身分証明体、1000 センタ装置、1001 入出力部、1

002 制御部、1003 データベース管理部、1004 変換部、1005 添付部、2000 認証側装置、2001 入出力部、2002 制御部、2003 変換部、2004 リモート検索部、5000 身分証明体、6000 ネットワーク

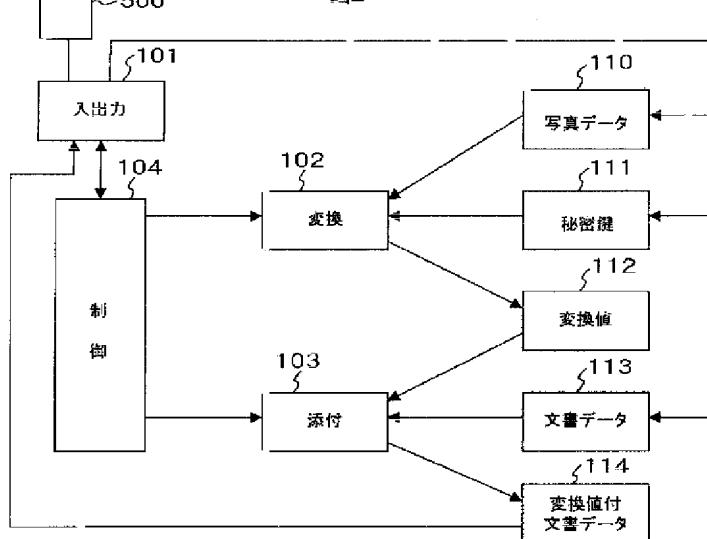
【図1】

図1



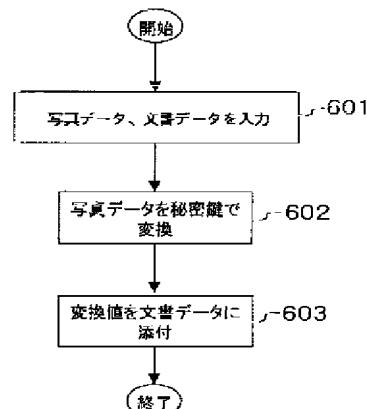
【図2】

図2



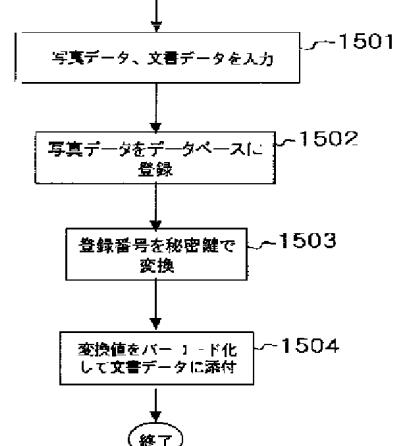
【図6】

図6



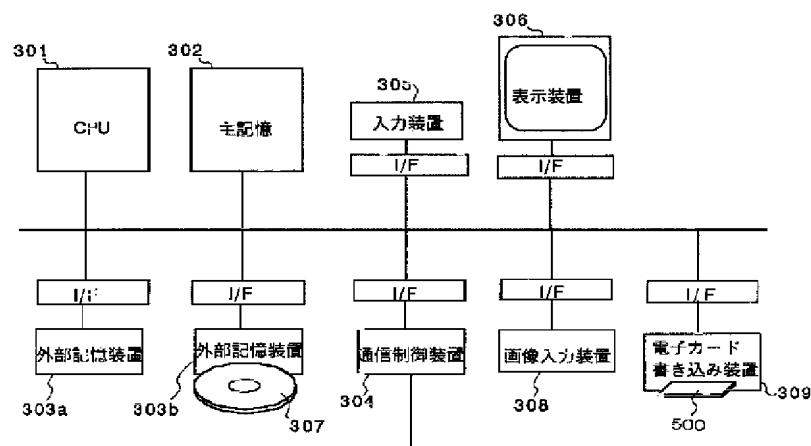
【図15】

図15



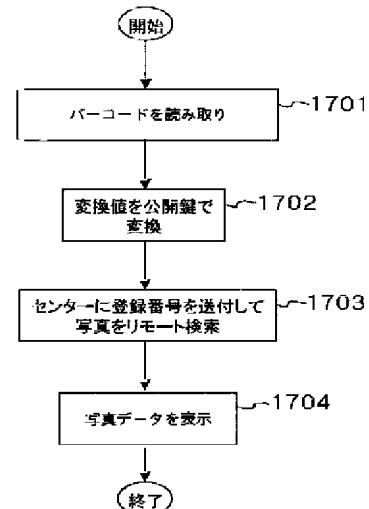
【図3】

図3



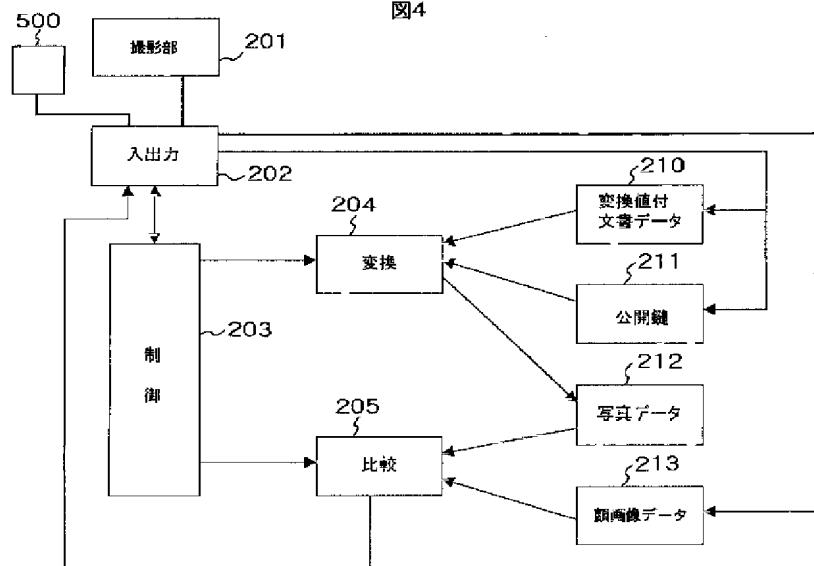
【図17】

図17



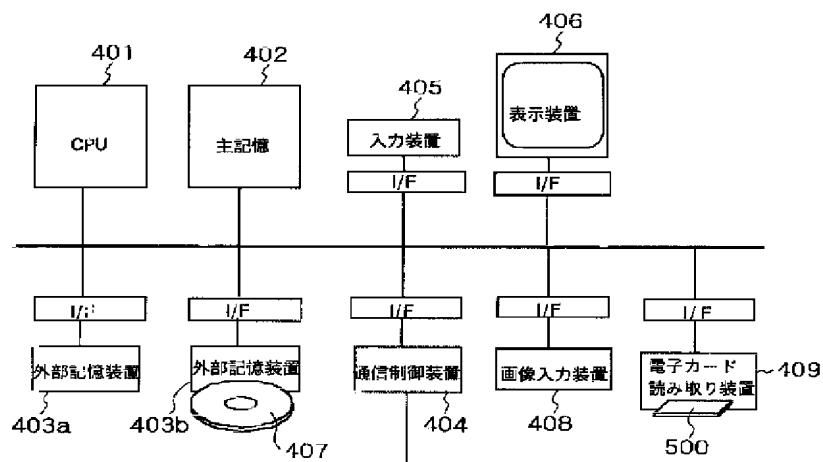
【図4】

図4



【図5】

図5

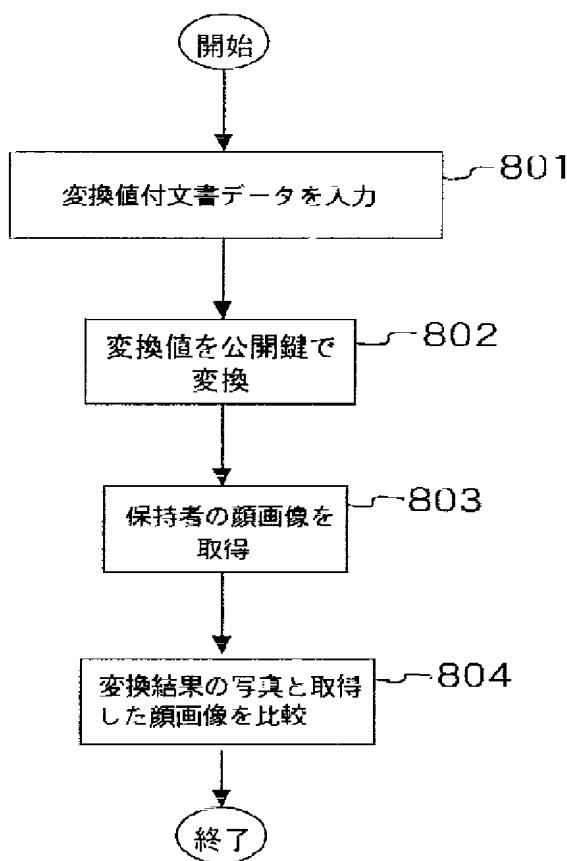
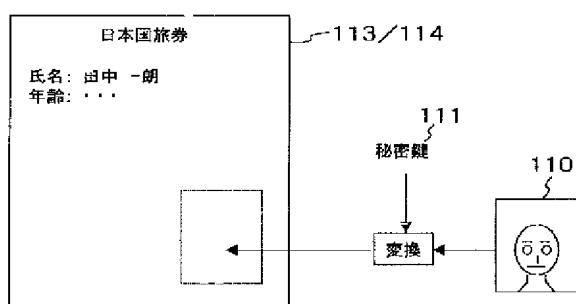


【図7】

【図8】

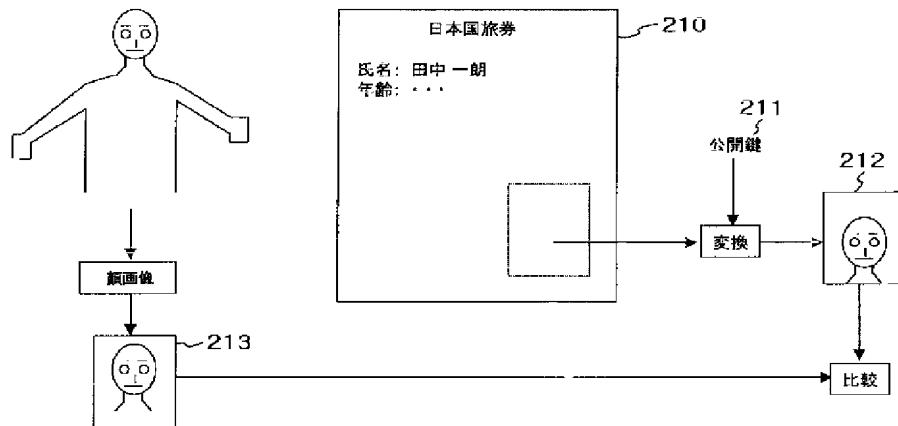
図7

図8



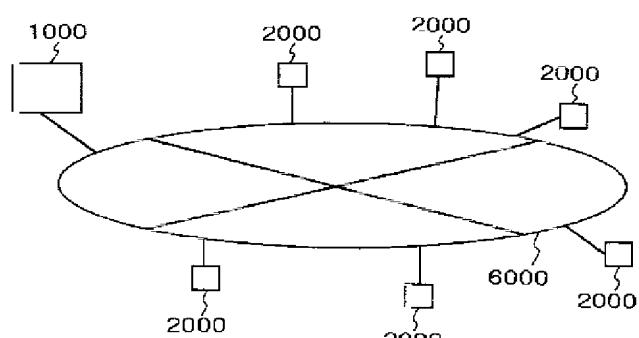
【図9】

図9



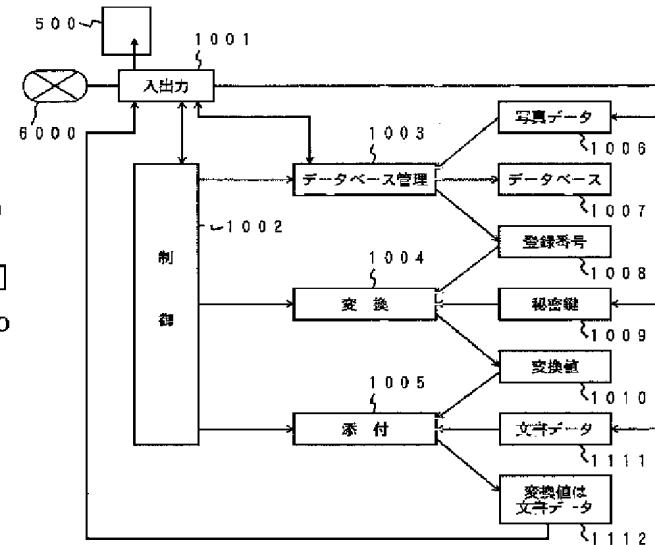
【図10】

図10



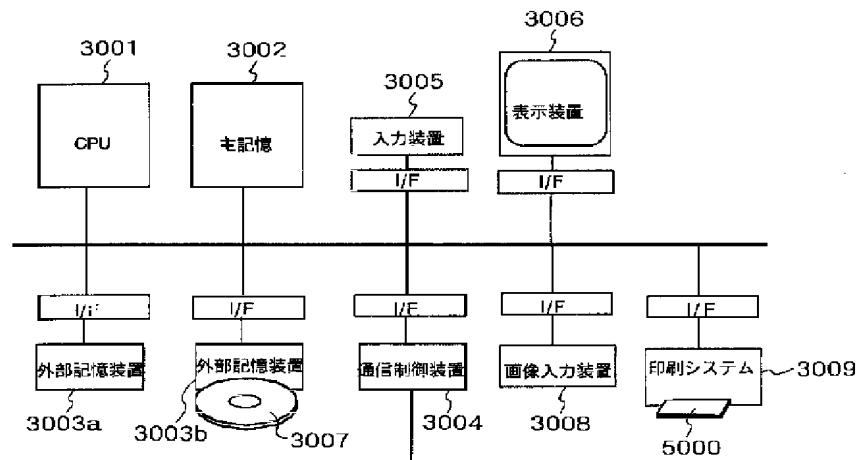
【図11】

図11



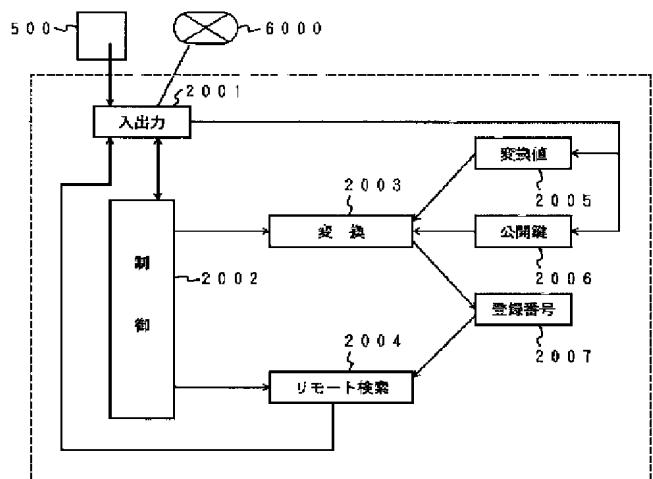
【図12】

图12



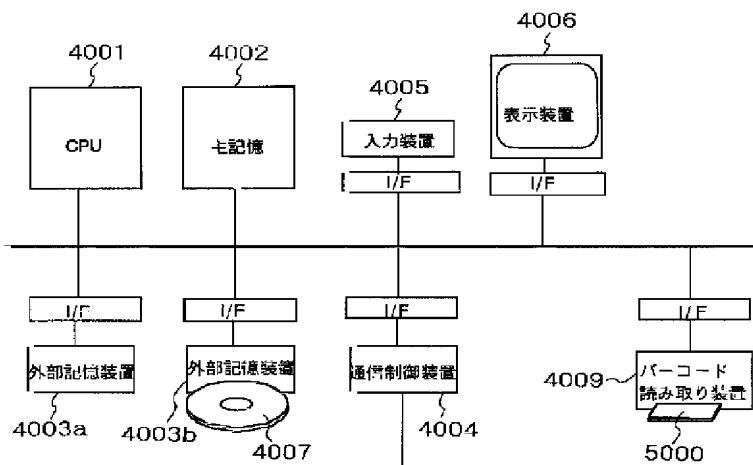
【図13】

図13



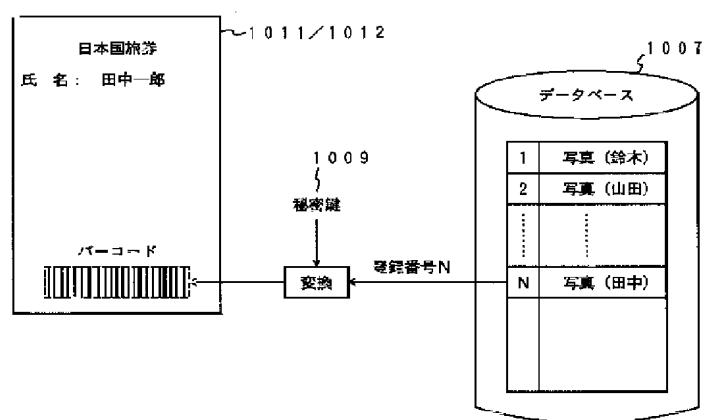
【図14】

図14



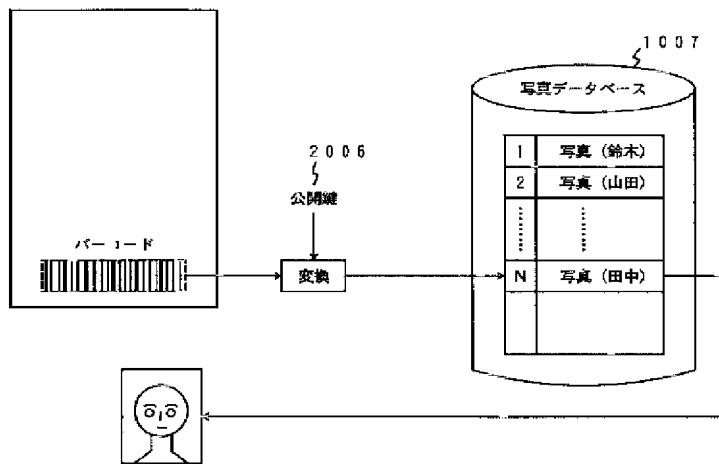
【図16】

図16



【図18】

図18



フロントページの続き

F ターム(参考) 2C005 HA01 HB02 JA01 JA15 JA26
JB02 JB06 JB33 JB40 LA33
LB32 LB34
5B085 AE12 AE13 AE23 AE25 AE29
5J104 AA07 AA13 KA01 KA05 NA38
PA14
9A001 BB03 BB04 DD13 EE03 FF03
HH21 HH34 JJ01 KK42 LL03